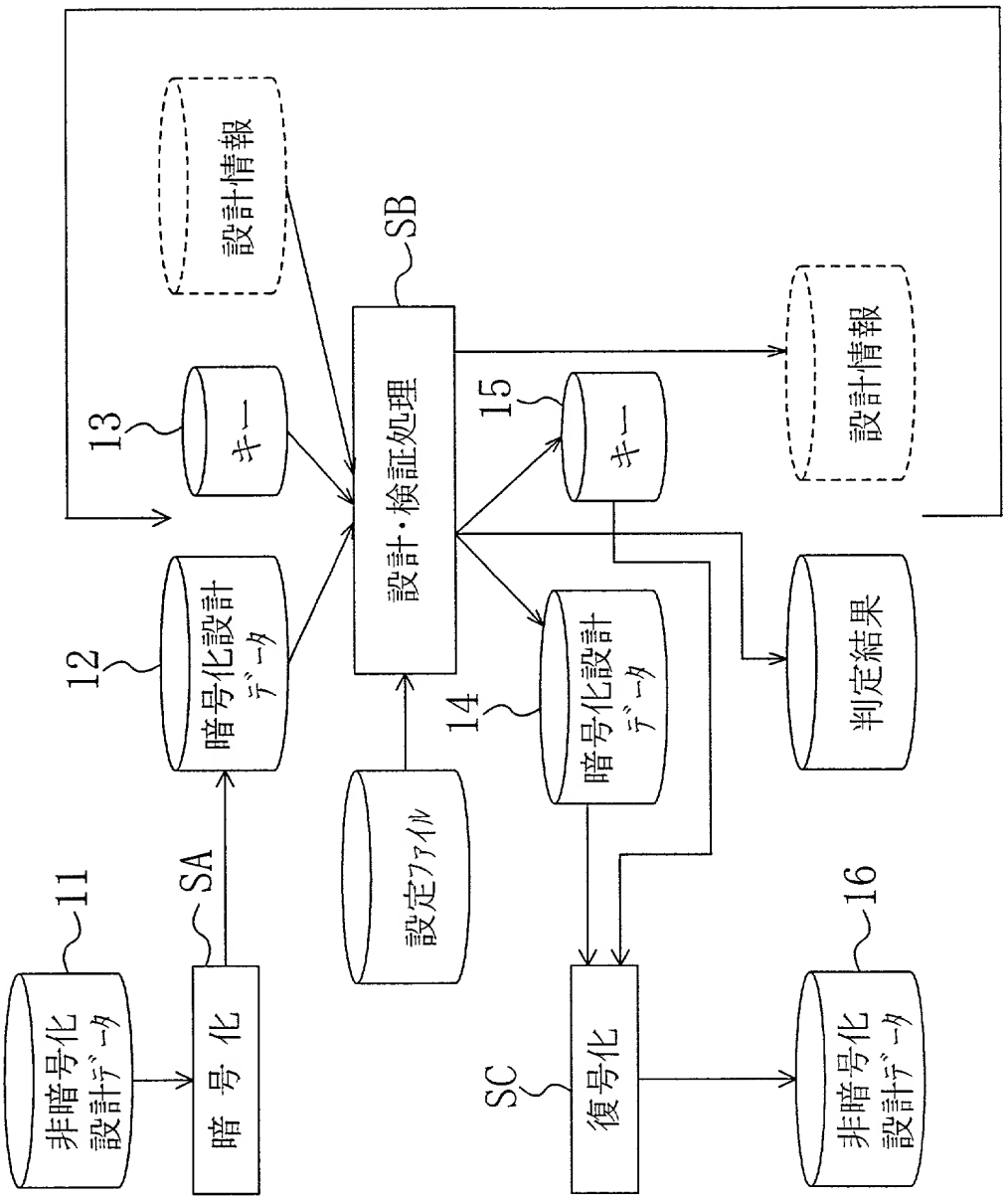
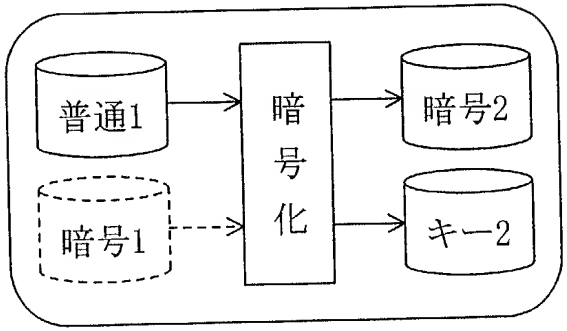
図1

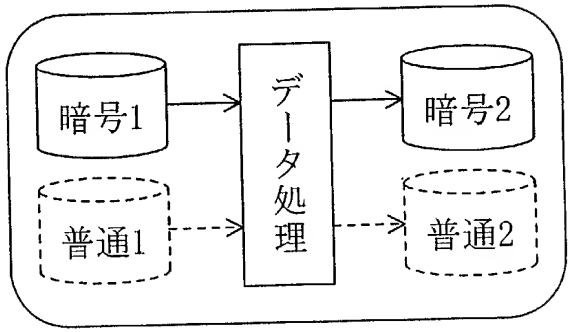

非暗号化設計データ
11
暗号化
SA
暗号化設計データ
12
キー
13
設計情報
設計・検証処理
SB
設定ファイル
暗号化設計データ
14
キー
15
設計情報
判定結果
復号化
SC
非暗号化設計データ
16

A



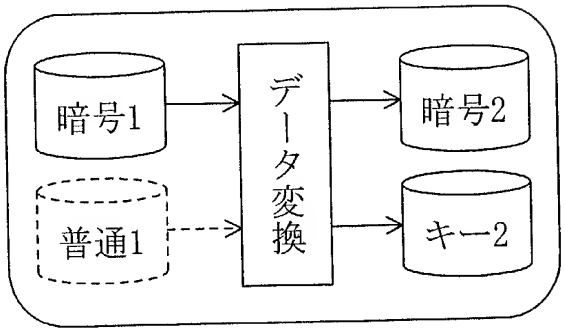
(a)

B１ 暗号ﾃﾞｰﾀのまま処理



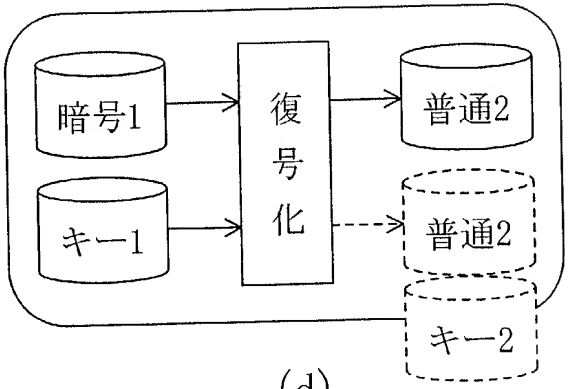
(b)

B２ 暗号を保ったﾃﾞｰﾀ変換



(c)

C



(d)

図2

EP0603707 Claims of 2650

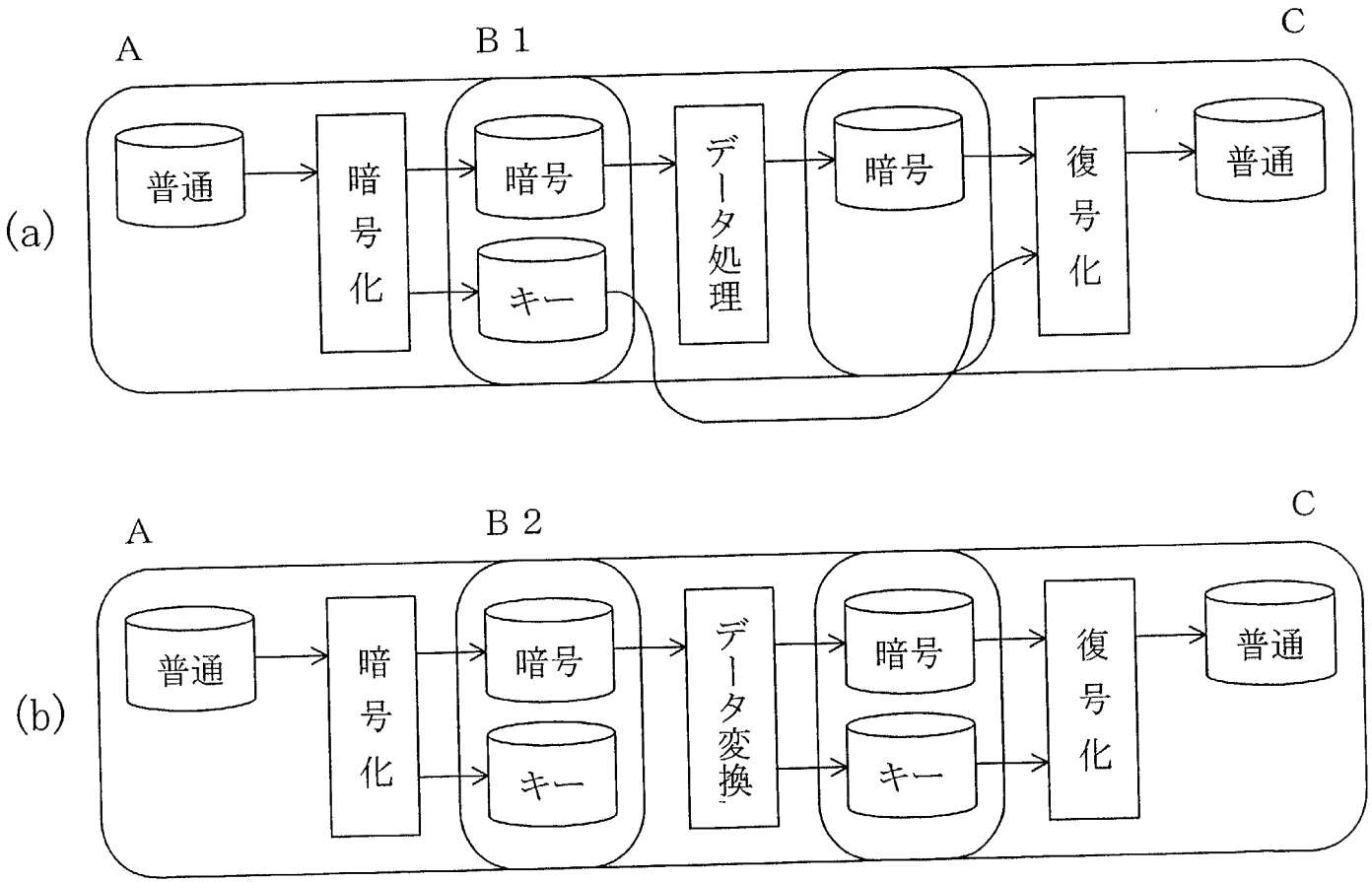
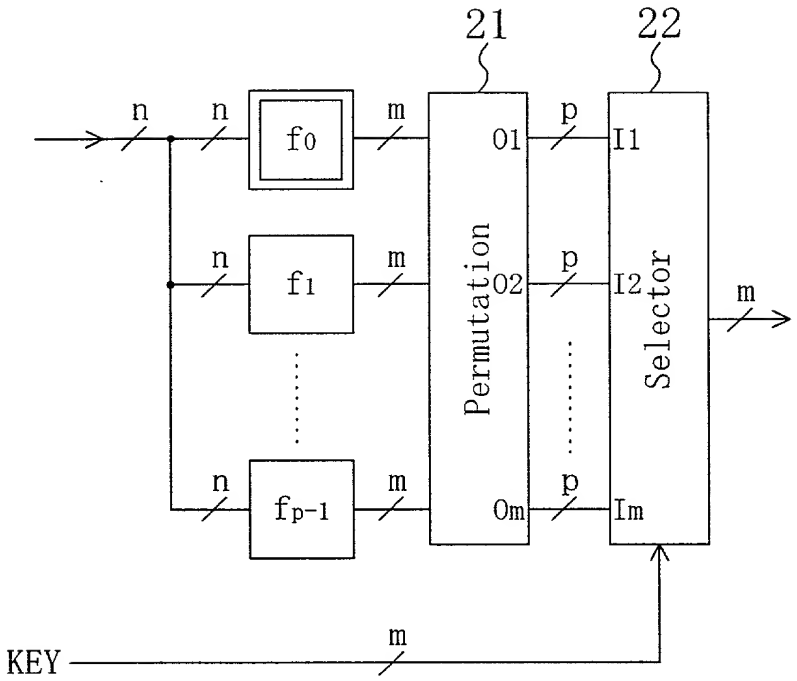


図3

図4


21
22
n
n
f0
m
01
p
I1
n
f1
m
02
I2
m
Permutation
Selector
n
fp-1
m
0m
Im
KEY
m

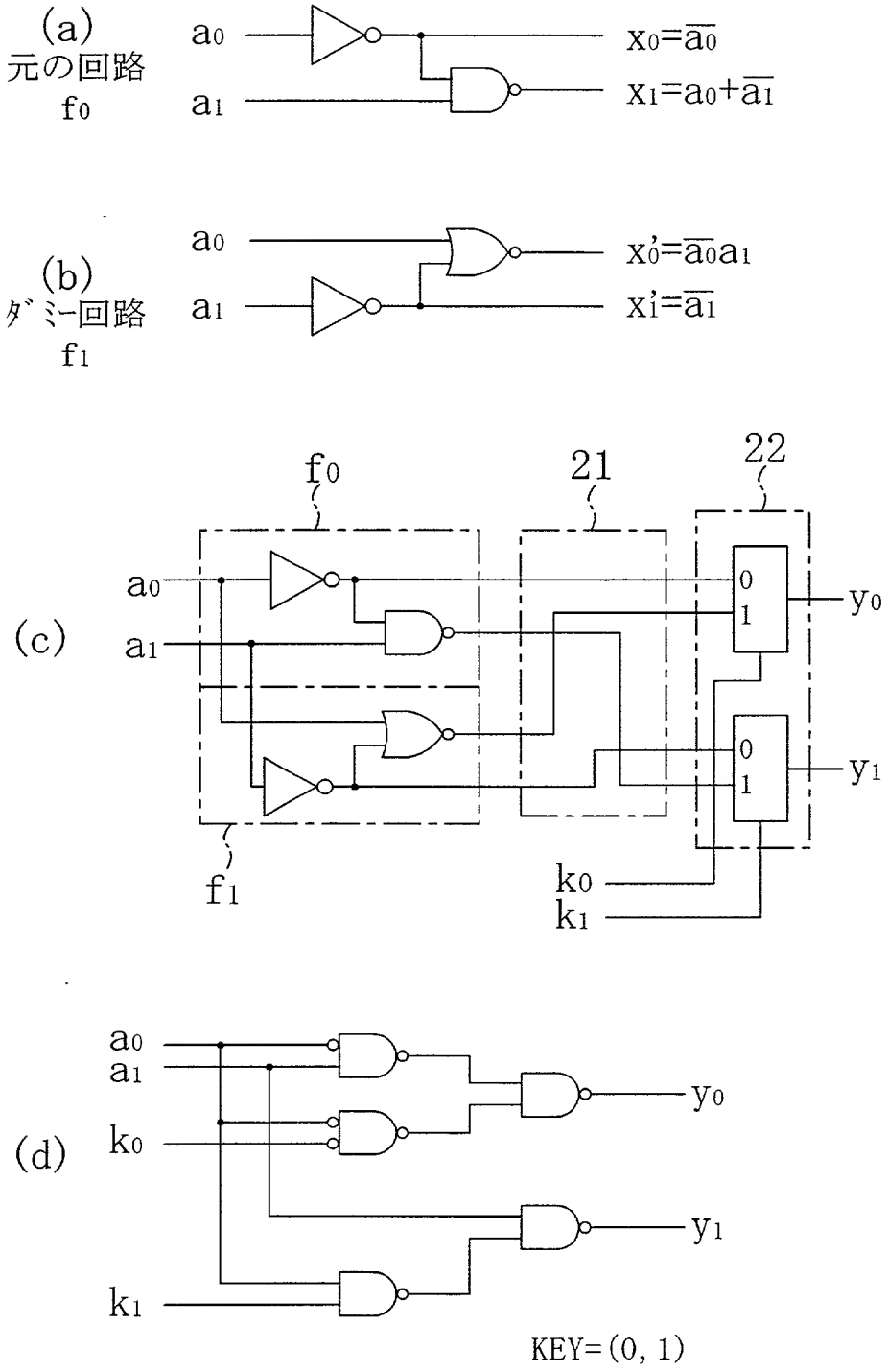

(a)
元の回路
f0
a0
a1
x0=ā0
x1=a0+ā1
(b)
ダミー回路
f1
a0
a1
x'0=ā0a1
x'1=ā1
(c)
f0
21
22
a0
a1
0
1
y0
y1
f1
k0
k1
(d)
a0
a1
k0
k1
y0
y1
KEY=(0, 1)

図6

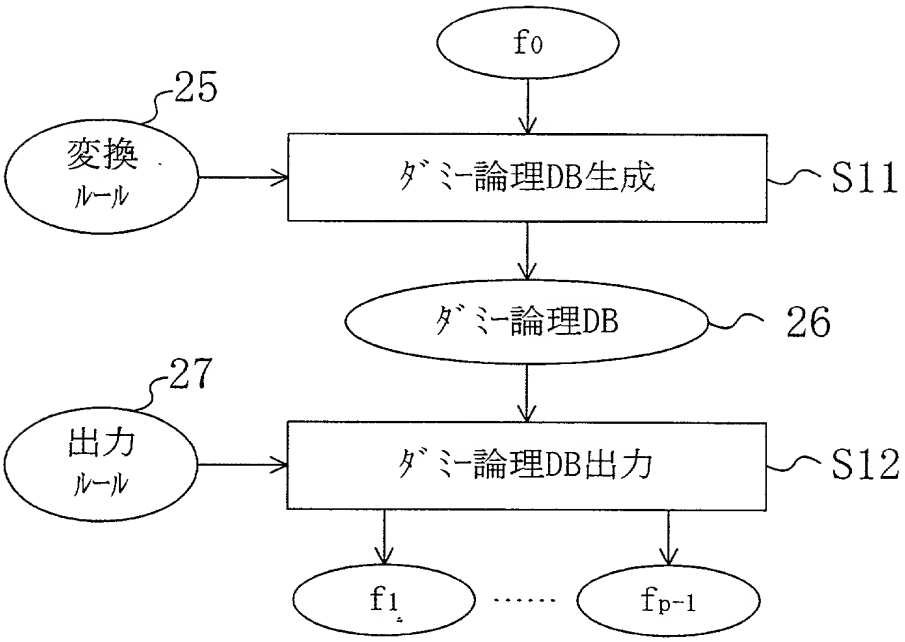

f0
25
変換
ルール
ダミー論理DB生成
S11
ダミー論理DB
26
27
出力
ルール
ダミー論理DB出力
S12
f1
……
fp-1

図7

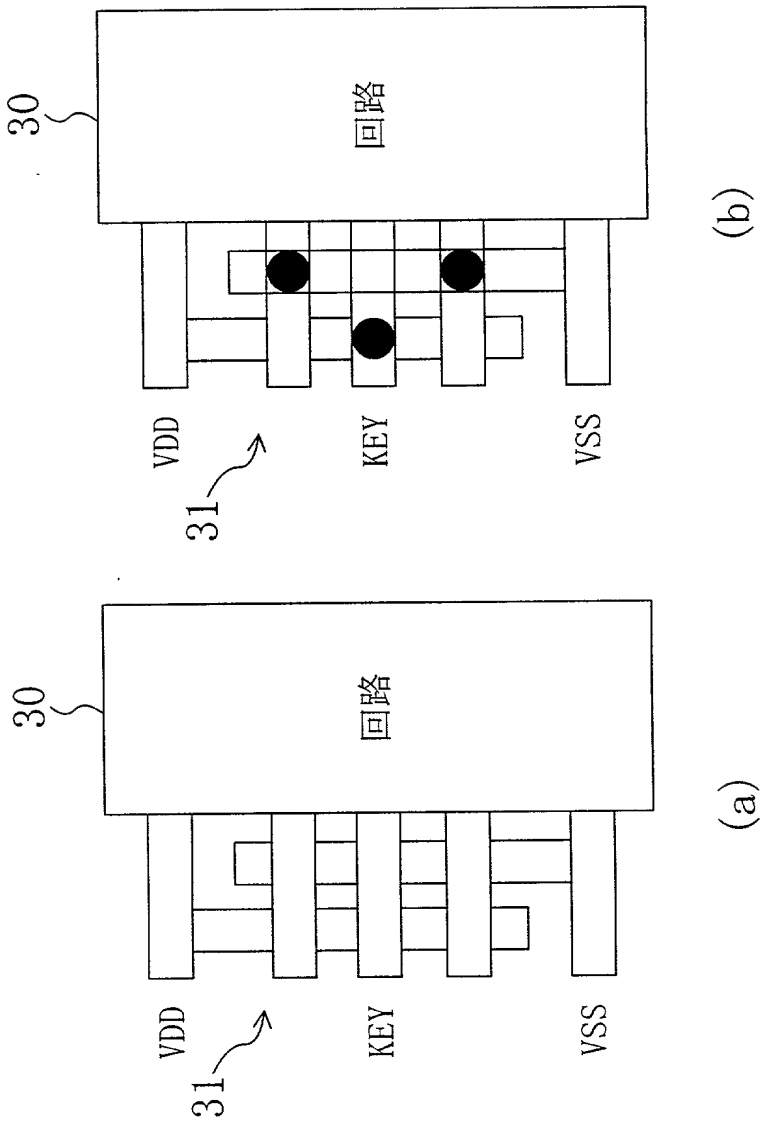


図8

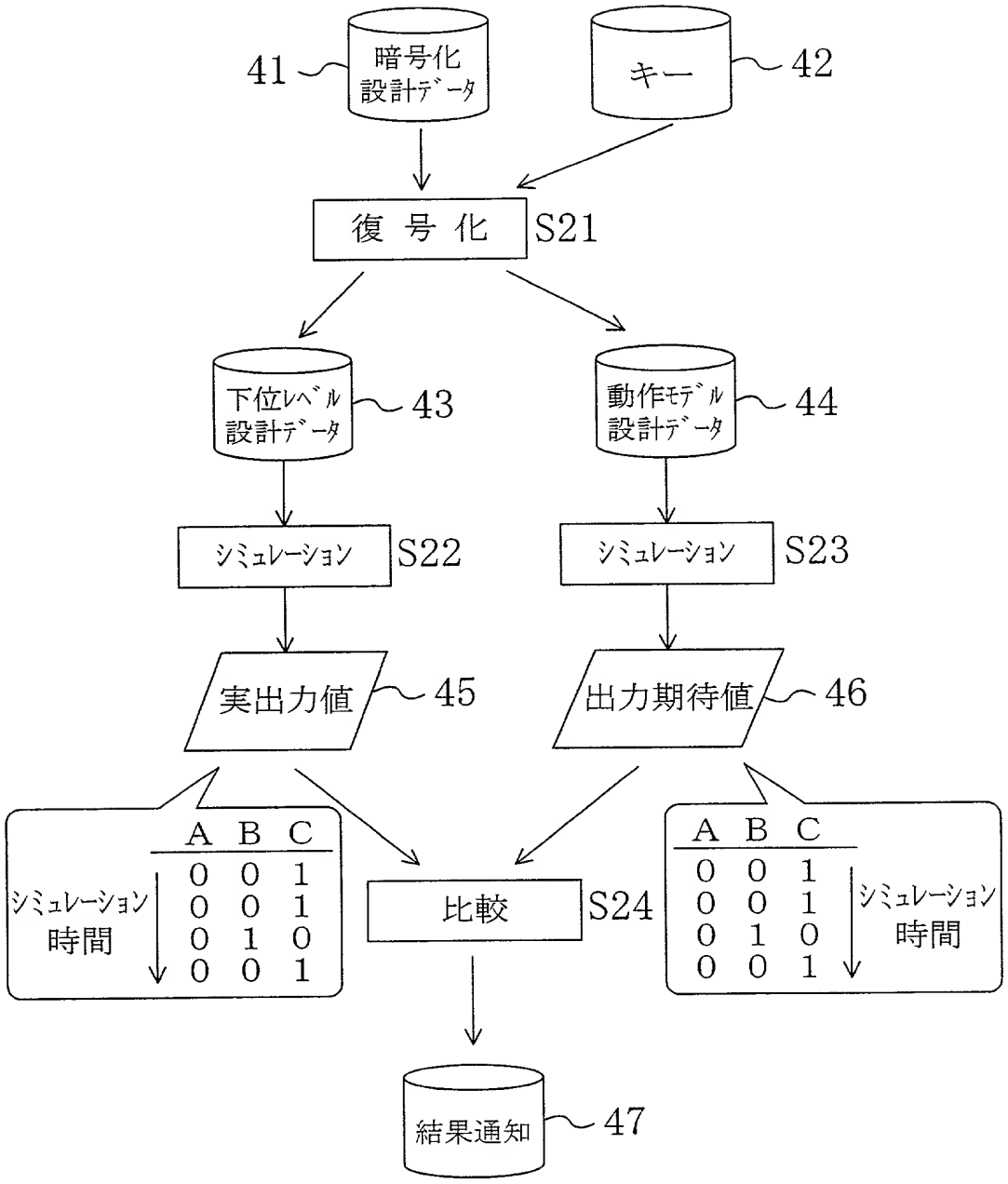
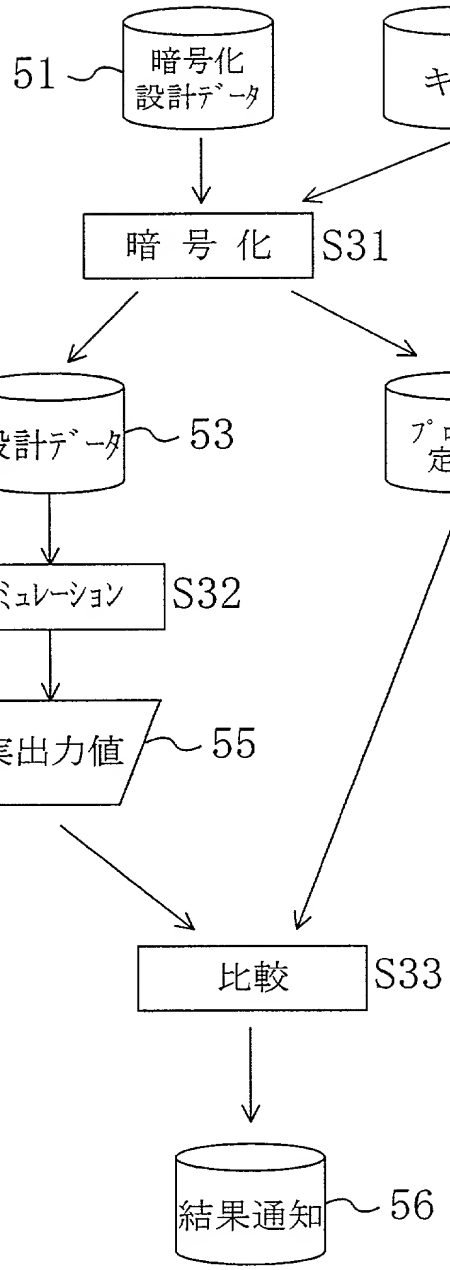
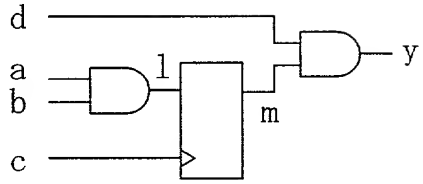

41
暗号化
設計ﾃﾞｰﾀ
キー
42
復 号 化
S21
下位ﾚﾍﾞﾙ
設計ﾃﾞｰﾀ
43
動作ﾓﾃﾞﾙ
設計ﾃﾞｰﾀ
44
シミュレーション
S22
シミュレーション
S23
実出力値
45
出力期待値
46
A B C
0 0 1
0 0 1
0 1 0
0 0 1
シミュレーション
時間
比較
S24
A B C
0 0 1
0 0 1
0 1 0
0 0 1
シミュレーション
時間
結果通知
47

図9



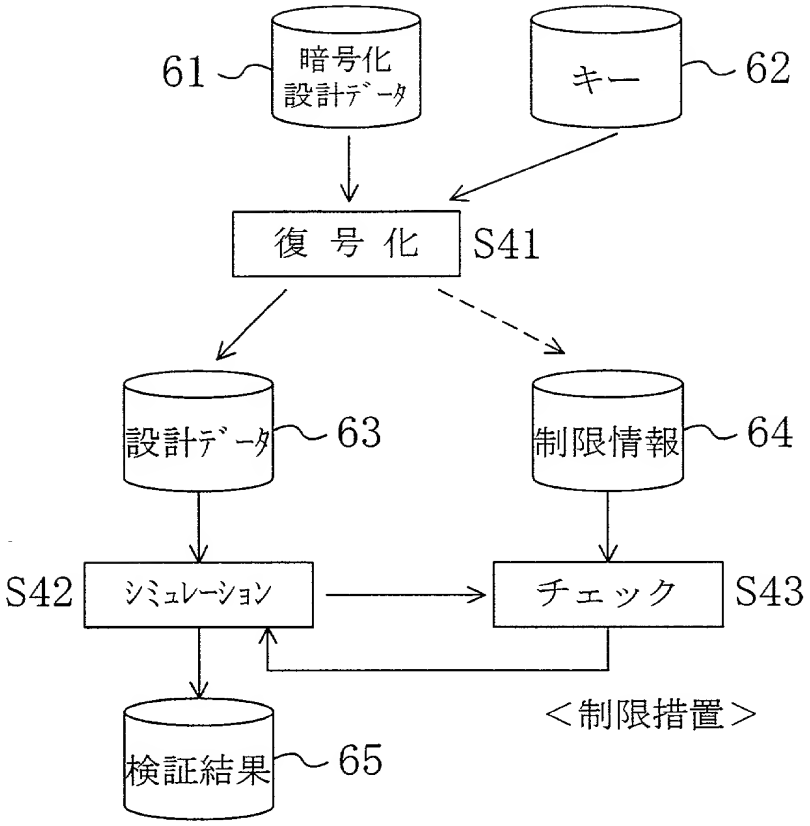
<設計データ>



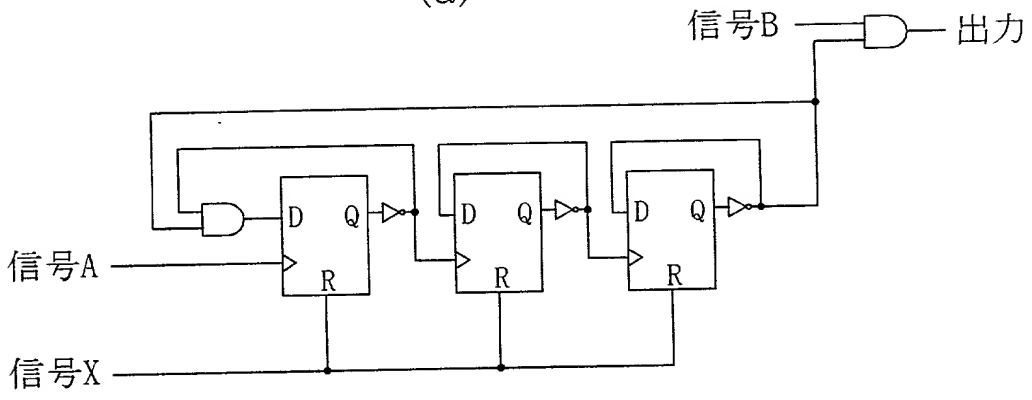
<プロトコル定義>

a	b	c	d	l	m	y
0	0	0	0	0	Q_{n-1}	0
1	0	0	0	0	Q_{n-1}	0
0	1	0	0	0	Q_{n-1}	0
1	1	0	0	1	Q_{n-1}	0
0	0	1	0	0	0	0
⋮				⋮		

図10


61
暗号化
設計データ
キー
62
復号化
S41
設計データ
63
制限情報
64
S42
シミュレーション
チェック
S43
＜制限措置＞
検証結果
65

(a)

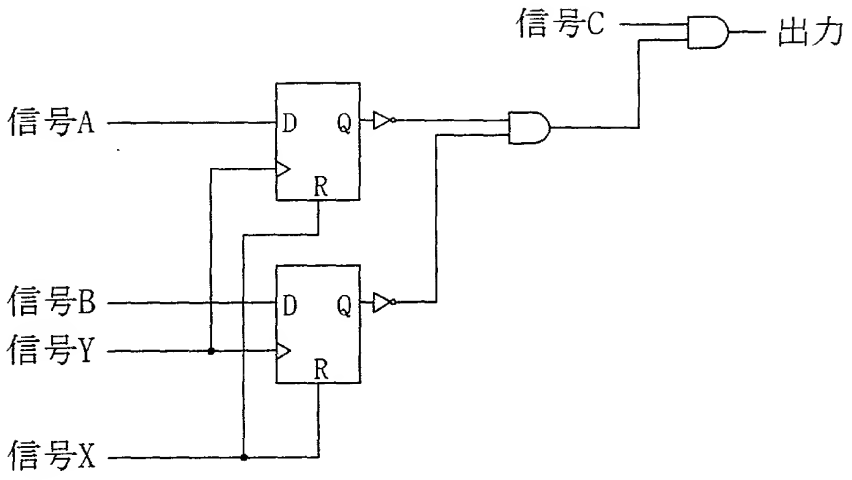


(b)

X	Aの変化回数	B	出力	
0	1	0	0	OK
		1	1	
0	2	0	0	OK
	⋮	1	1	
			⋮	
0	7	0	0	OK
		1	1	
0	8	0	0	NG
		1	0	
0	9	0	0	NG
	⋮	1	0	
			⋮	

図12

(a)



(b)

X	Y	A	B	C	出力	
0	↑	0	0	0	0	OK
		0	0	1	1	
		0	1	0	0	NG
		0	1	1	0	
		1	0	0	0	
		1	0	1	0	
		1	1	0	0	
		1	1	1	0	

図13

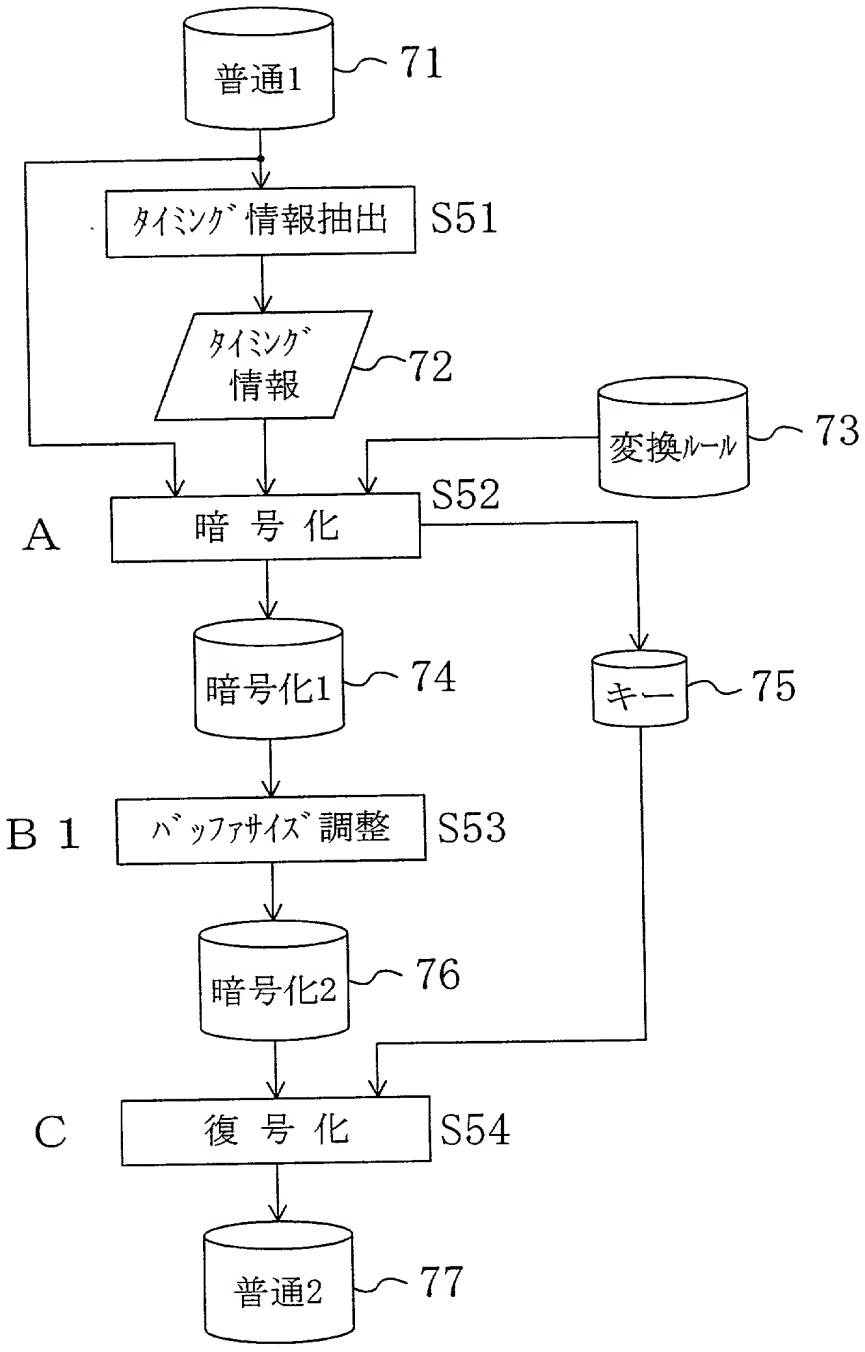

普通1
71
タイミング情報抽出
S51
タイミング情報
72
変換ルール
73
A
暗号化
S52
暗号化1
74
キー
75
B1
バッファサイズ調整
S53
暗号化2
76
C
復号化
S54
普通2
77

図14

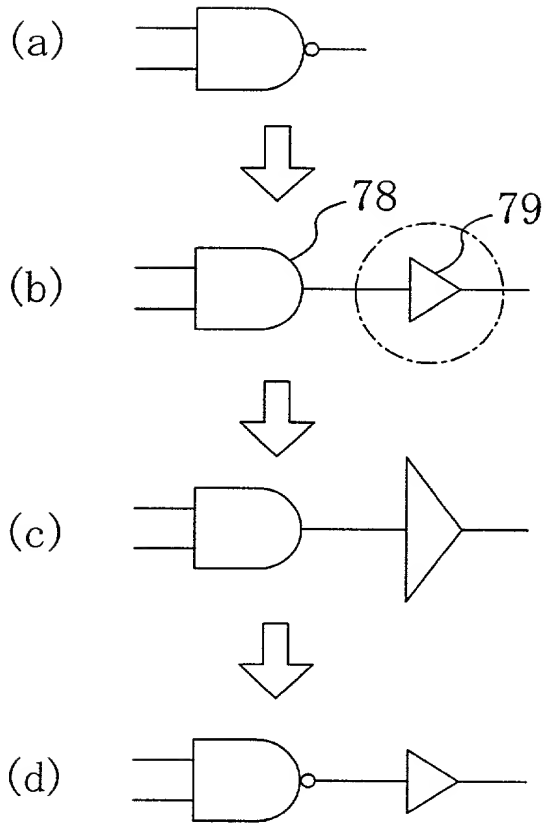
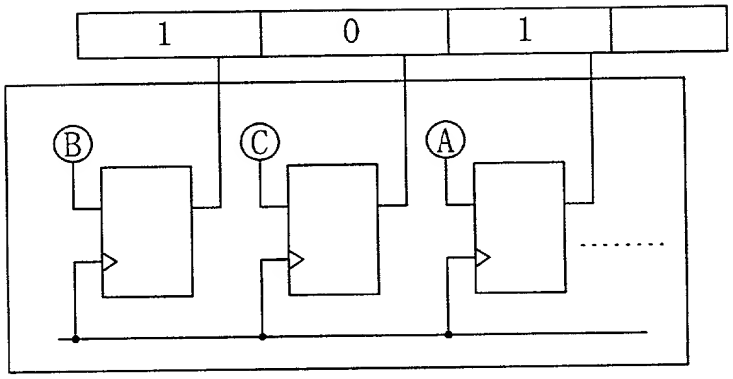


図15

回路固有IDﾚｼﾞｽﾀ



A＝1
B＝1
C＝0
} 固有ﾊﾟﾗﾒｰﾀ

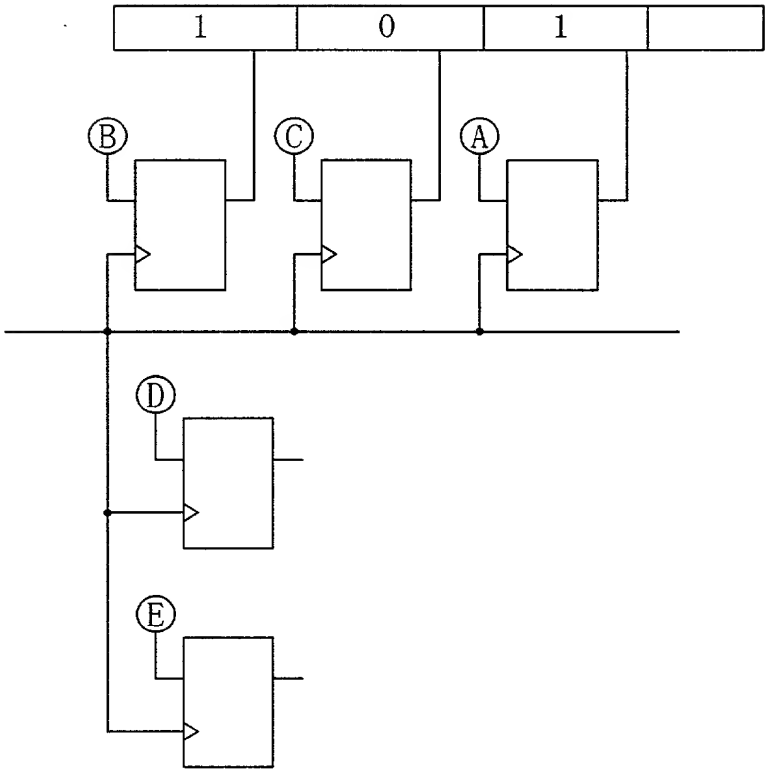



図16